Department of Homeland Security Daily Open Source Infrastructure Report for 17 April 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The New York Times reports that there is increasing evidence that a thriving international trade in smuggled poultry is helping spread bird flu. (See item 27)
- The U.S. Centers for Disease Control and Prevention reports that the Iowa Department of Public Health has identified two persons diagnosed with mumps who were potentially infectious during travel on nine different commercial flights involving two airlines between March 26 and April 2. (See item 28)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: **Energy**; **Chemical Industry and Hazardous Materials**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation and Border Security**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information Technology and Telecommunications**; **Internet Alert Dashboard**

Other: **Commercial Facilities/Real Estate, Monument &Icons**; **General**; **DHS Daily Report Contact Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 14, Associated Press* — **Coal industry is on the rebound in Ohio.** With the skyrocketing cost of oil and new pollution controls, coal is on the rebound. Mines are being reopened and new miners are being hired. Demand for U.S. coal is expected to be a record 1.2 billion tons this year, up from 1.18 billion in 2005, according to the National Mining Association. Production is forecast to be 1.16 billion tons, a 3.2 percent increase over 2005. Sixty−nine mines opened in Appalachia last year, according to the U.S. Energy Information Administration. Many credit coal's revival to it being seen as an alternative to increasingly expensive oil and natural gas. Others point to the binge in construction of −− or plans for −−

new coal−fired power plants to satisfy the nation's surging demand for electricity. There are about 100 mines and 35 coal companies in Ohio. An estimated 24.6 million tons of coal were mined last year by the state's 2,500 mine workers. That's up from 23.5 million tons in 2004 and 22.3 million tons in 2003, when there were 2,300 workers.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/14/AR2006041400812_pf.html

2. *April 14, Aberdeen News (SD)* — **Gunfire damages electrical transformer.** A substation transformer near Sisseton, SD, sustained gunshot damage earlier this month, temporarily cutting power to hundreds of customers and requiring an Environmental Protection Agency (EPA) cleanup crew. According to a sheriff's department release, on Thursday, April 6, several gunshot holes were discovered in a substation transformer north of Sisseton. The 21 shots caused approximately 900 to 1,000 gallons of oil to leak onto the ground. The oil leak caused the transformer to fail and left about 600 customers in Sisseton without power for a short time. The oil spill required a cleanup crew from the EPA. Damage estimates at this time are between $25,000 and $50,000.
Source: http://www.aberdeennews.com/mld/aberdeennews/news/14341004.htm?source=rss&channel=aberdeennews_news

3. *April 13, Canadian Broadcasting News* — **U.S. will be told to keep tankers out of Canadian waters: MP.** Canada is prepared to go to court to try to keep the U.S. from allowing liquefied natural gas tankers to use a dangerous stretch of a bay in southern New Brunswick. At issue is whether Canada can legally bar commercial ships from using a Canadian waterway to reach a U.S. port. Ships have the right to "innocent passage" through internal waterways, but Greg Thompson, a conservative MP of New Brunswick Southwest, says the hazard of a natural gas spill makes the tankers' passage far from innocent in this case.
Source: http://www.cbc.ca/story/canada/national/2006/04/13/lng−passamaquoddy060413.html?ref=rss

4. *April 13, Canadian Broadcasting Corporation* — **Chemists find more efficient coal−to−diesel conversion.** U.S. scientists say they have found a way to boost the efficiency of a 90−year−old method of converting coal into synthetic diesel fuel. The two−step chemical process, developed by chemists at Rutgers University in New Jersey and the University of North Carolina at Chapel Hill, converts some of the waste product from the original process into usable diesel. The researchers said their work could reduce U.S. dependence on oil imports for its energy reserves. They added that their research is still in the early stages, and improvements to their methods are needed before they can be put into practice. The Fischer−Tropsch process for making synthetic fuels from carbon sources such as coal was invented by German chemists in 1920. It is considered too inefficient and too expensive to compete with traditional oil refining. The new process, described in a recent issue of the journal Science, uses two catalysts to convert medium−weight hydrocarbons into useful products. The researchers say the reactions involved in their new process are selective and create usable molecules from the medium−weight hydrocarbons that used to be considered byproducts.
Source: http://www.cbc.ca/story/science/national/2006/04/13/coal−die sel−20060413.html

5. *April 13, U.S. Department of Energy* — **DOE seeks industry proposals for feasibility study to produce hydrogen at existing nuclear power plants.** In support of President Bush’s

Advanced Energy Initiative, Secretary of Energy Samuel W. Bodman on Thursday, April 13, announced that the Department of Energy will allocate up to $1.6 million this year to fund industry studies on the best ways to utilize energy from existing commercial nuclear reactors for production of hydrogen in a safe and environmentally−sound manner. Secretary Bodman said, “Hydrogen is a key component of our energy future, and developing this clean source through our nuclear reactors will help reduce America’s dependence on foreign sources of energy.” The department proposes to partner with industry on the feasibility studies on hydrogen production using small−scale equipment at existing commercial nuclear reactors for up to three years to examine the economic implications of producing hydrogen in this way, the environmental effects, and the regulatory requirements. This activity helps advance the goals for production of hydrogen using nuclear power, which were expressed in the Energy Policy Act of 2005.
Additional information on the Nuclear Hydrogen Initiative: http://www.nuclear.gov/
Source: http://www.energy.gov/news/3480.htm

6. *April 13, Monroe News (MI)* — **Loose nut prompts Fermi 2 generator dismantling.** Workers are dismantling the main generator at the Detroit Edison Co.'s Fermi 2 nuclear power plant after a routine inspection revealed a metal nut fused between the rotor and the stator of the big machine. The plant has been idled for refueling and maintenance since Saturday, March 25. Officials said it's not a nuclear or safety issue because the generator is on the non−nuclear side of the plant, separate from the nuclear reactor itself. The dismantling of the generator is to ensure that nothing else inside of it is associated with the loose nut and to make sure the generator is not damaged. The Fermi plant is in the midst of what is expected to be a 30−day shutdown while a third of the reactor's nuclear core is replaced and other maintenance work is performed.
   Source: http://www.monroenews.com/apps/pbcs.dll/article?AID=/20060413/NEWS01/104130005/−1/NEWS

[Return to top]

Chemical Industry and Hazardous Materials Sector

7. *April 14, Honolulu Advertiser* — **Pesticide fumes sicken schoolchildren.** A pesticide sprayed in a yard across the street from 'Aina Haina Elementary School sent more than 40 students to five Honolulu hospitals Thursday afternoon, April 13, for observation. Aside from one child who vomited as a result of the pesticide fumes, the worst symptoms were nausea and watery, itchy eyes, said Greg Knudsen, spokesperson for the state Department of Education. None of the school children were seriously ill, he said. The children were kept after school longer than usual to ensure that enough time had passed for the fumes to dissipate, Knudsen said.
   Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20060414/NEWS01/604140362/1190/NEWS

[Return to top]

Defense Industrial Base Sector

8. *April 14, Aviation Now* — **Air Force strives for better IT savings.** The U.S. Air Force is eyeing more of a service−wide information technology acquisition strategy to bridge East and West Coast industries, as well as push for greater cost savings, Ronald A. Poussard, Air Force Program Executive Officer for Combat and Mission Support Services, said Thursday, April 13. Poussard, speaking to the Armed Forces Communications and Electronics Association's Washington, DC, chapter, said the "synergies" produced also could push industry to get involved in "shaping" IT project requirements quicker, but could lead to greater programmatic delays at the same time. He said contract vehicles in which the government assumes virtually all of the risk are inefficient. Still, industry should be rewarded for creative solutions. Meanwhile, a recent policy memorandum said award fees and incentives will be rewarded for going "above and beyond," and performance will be measured at "zero and going up, not 100 and going down." Poussard credited a "perfect storm" of decreasing budgets and personnel for the latest top−level Air Force push for IT acquisition reform.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/AFIT04146.xml

9. *April 14, USA Today* — **The new breed of soldier: Robots with guns.** Spurred by the risks from roadside bombs and terrorist ambushes, the military is aggressively seeking to replace troops with battlefield robots, including new versions armed with machine guns. Although the Pentagon initially focused on aircraft, such as the Predator drone, now new ground− and sea−based robots are being developed and tested. To better detect and stop improvised explosive devices, new sensors are being attached to those robots. The military also is responding to some creative tinkering by the troops, who have modified their robots to carry grenades and other weapons into buildings or other potentially unsafe targets. As a result, the Pentagon is testing a new version of the Talon robot that carries a remote−control M−240 machine gun. Meanwhile, much larger and more ambitious robot weapons are in testing, including a tank−like, 1,600−pound vehicle called the Gladiator, which can fire a variety of guns, tear gas or almost anything else that fits.
Source: http://www.usatoday.com/tech/news/techinnovations/2006−04−13−robot−soldiers_x.htm?POE=TECISVA

10. *April 14, Government Accountability Office* — **GAO−06−368: Defense Acquisitions: Major Weapon Systems Continue to Experience Cost and Schedule Problems Under DoD's Revised Policy (Report).** The Department of Defense (DoD) is planning to invest $1.3 trillion between 2005 and 2009 in researching, developing, and procuring major weapon systems. How DoD manages this investment has been a matter of congressional concern for years. Numerous programs have been marked by cost overruns, schedule delays, and reduced performance. Over the past three decades, DoD’s acquisition environment has undergone many changes aimed at curbing cost, schedule, and other problems. In order to determine if the policy DoD put in place is achieving its intended goals, the Government Accountability Office (GAO) assessed the outcomes of major weapons development programs initiated under the revised policy. Additionally, GAO assessed whether the policy’s knowledge−based, evolutionary principles are being effectively implemented, and whether effective controls and specific criteria are in place and being used to make sound investment decisions. GAO recommends that DoD insert specific criteria into the policy at key investment points and require programs satisfy those criteria before allowing them to move forward. In order to insure transparency and accountability, GAO also recommends that DoD require decision makers to include the

rationale for their decisions in decision documentation. DoD partially concurred with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06368high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−368

[Return to top]

Banking and Finance Sector

11. *April 14, Websense Security Labs* — **Phishing Alert: Oregon Community Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Oregon Community Credit Union. Users receive a spoofed e−mail message, which claims that their e−mail address needs to be verified in order to keep up to date with important announcements. The message provides a link to a phishing Website. Users who visit this Website are prompted to enter account information, including account number, account password, and ATM card details.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =463

12. *April 14, Daily Breeze (CA)* — **Ring of alleged ID thieves cast wide net across U.S.** Police on Thursday, April 13 said they had broken a Southern California identity theft ring that victimized scores of people, some living as far away as Florida. Police announced charges against 20 people suspected of stealing identities to create fake checks and credit cards, and setting up phony businesses to swipe stolen credit card numbers. The crackdown began about eight months ago when a single counterfeit check was passed at a bank in San Pedro, CA. A trail led to an elaborate organized−crime ring that committed millions of dollars in fraud, police said. Scores of people and banking institutions were victimized. About $2 million in fraud allegedly occurred in 2005 alone, but the ring is believed to have been around since 2000. Prosecutors filed 97 felony charges against the suspects for offenses including conspiracy, identity theft, false financial statements, and receiving stolen property.
Source: http://www.dailybreeze.com/news/articles/2633496.html?showAl l=y&c=y

13. *April 14, News 4 Hawaii Channel (HI)* — **Thousands of Hawaii workers exposed to possible identity theft.** The Hawaii Attorney General's Office alerted more than 40,000 Hawaii residents Thursday, April 13, that they are at risk for identity theft. This includes 22,000 private sector employees, and more than 21,000 members of the Hawaii Government Employees Association and the United Public Workers Union. The warning comes after the U.S. Secret Service and Postal Inspection Service notified the state attorney general of the theft of insurance company records. Those records include a list of names and Social Security numbers of people enrolled in certain health and group life insurance plans in 1999. The Honolulu Police Department found the copied records on a computer that was being used by a suspect under investigation for drug crimes. Information regarding spouses and dependent children were not included in the stolen lists. Federal officials first informed the Attorney General's office of the theft in January. The incident has not been disclosed publicly until now because it would have impaired the federal investigation.
Source: http://news.yahoo.com/s/kitv/20060414/lo_kitv/3400180

14. *April 13, Websense Security Labs* — **Phishing Alert: Corporate America Family Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Corporate America Family Credit Union. Users receive a spoofed e−mail message, which claims that they should log on to the secure online banking system to safeguard and protect against possible unauthorized access. Users are asked to update their contact e−mail to ensure that they receive important announcements. The message provides a link to a phishing Website. Users who visit this Website are prompted to enter personal and account information, such as user name, password, and ATM pin.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =462

[Return to top]

Transportation and Border Security Sector

15. *April 16, Scripps Howard News Service* — **Massive California ports, rail and highway plan nears agreement.** Every day, the 300−foot cranes at the Port of Los Angeles remove containers of toys, clothes, and other goods from Asian ships and place them on American trucks and trains for delivery to consumers around the country. At the Los Angeles port and the neighboring Port of Long Beach, these cranes handle 40 percent of all shipments to the U.S., making this the largest port complex in the nation and the fifth largest in the world. Trade through the two ports generates some 500,000 jobs, and the number of jobs could double over the next 25 years, according to the Southern California Association of Governments. Economists and port advocates say the future of these jobs and the state's economy, however, depend on Californians paying for new freeways, rail lines and other transportation improvements to keep goods moving quickly to market and trade growing. Those onshore improvements hinge on the closed−door negotiations between legislative leaders and the governor over bond plans to finance levees, roads, education and other public works. The $222 billion plan Governor Arnold Schwarzenegger unveiled in January included $15 billion in rail improvements, roads and other port−related public works.
Source: http://www.shns.com/shns/g_index2.cfm?action=detail&pk=PORT− 04−16−06

16. *April 15, BBC News* — **Passengers' air hoax ordeal ends.** Passengers on a flight from London’s Luton Airport who were diverted to Glasgow Prestwick Airport in Scotland following a bomb hoax have finally arrived in Galway in the Irish Republic. Staff at the Dublin−based airline Aer Arann raised the alarm at about 10:30 p.m. BST on Friday, April 14, shortly after take−off. Crewmembers of Aer Arann Flight RE 508 were alerted by passengers when the word "bomb" and a picture of an arrow were scrawled on a seat table. The aircraft was diverted to Prestwick, escorted by two Royal Air Force jets, and the 53 passengers and crew disembarked safely. "A full search of the plane was carried out and nothing of note found," a spokeswoman said. Police later confirmed the message was a hoax.
Source: http://news.bbc.co.uk/2/hi/uk_news/4911296.stm

17. *April 14, The Star−Ledger (NJ)* — **Threat to Newark plane forces an evacuation.** A Continental Airlines plane bound for Costa Rica was evacuated at Newark Liberty International Airport on Thursday, April 13, after police received a telephone threat directed at the flight, but a search turned up nothing dangerous, authorities said.
Source: http://www.nj.com/news/ledger/jersey/index.ssf?/base/news−3/

1144990803306650.xml&coll=1

[Return to top]

Postal and Shipping Sector

18. *April 08, Aviation Week & Space Technology* — **Cargo shifts with fuel surcharges, airline reorganization.** Air cargo gateways continue to grow in the U.S., both in shipments and in facilities, but the many−faceted upheaval in the airline industry has left some small and midsize airports and even the occasional hub with plenty of room on freight pallets. A lot of factors have come into play against cargo growth, analysts say. High fuel prices and a skittish airline industry focused on lowering costs have contributed to a kind of malaise. Airlines have tended to consolidate cargo where they can, filling up airplanes at both ends of a trip, and tending to grow at key gateways where trucks take over. With the airlines in turmoil and reorganization, the mix of aircraft operating at airports has changed. Typically, airlines are downsizing aircraft, in some cases putting regional jets in place of mainline aircraft that had belly cargo capabilities, reducing overall freight capacity and cargo volume. The options shippers have today in choosing type of service −− overnight, one−day or two−day service for shipments −− favor trucks over more expensive but quicker air travel.
Source: http://www.aviationnow.com/avnow/news/channel_awst_story.jsp ?id=news/aw041006p1.xml

[Return to top]

Agriculture Sector

19. *April 14, Animal and Plant Health Inspection Service* — **Regulations for small lots of seed amended.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service has amended its regulations to allow the importation of small seed lots with import permits instead of phytosanitary certificates. This amendment will facilitate the safe import of small amounts of seed by individual importers, scientists, horticultural societies, arboreta and small businesses. These entities previously may have had difficulty obtaining the necessary import certificates and consequently were adversely affected by the phytosanitary certificate requirement. By removing the certificate requirement, this rule change will ensure prompt and consistent service for seed importers while continuing to protect against the introduction of plant pests into the U.S. The new seed import requirements will become effective May 15.
Source: http://www.aphis.usda.gov/newsroom/content/2006/04/seedpermi t.shtml

20. *April 14, University of Wisconsin−Madison* — **Soil−bound prions remain infectious.** Scientists have confirmed that prions, the mysterious proteins thought to cause chronic wasting disease (CWD) in deer, latch on tightly to certain minerals in soil and remain infectious. The discovery that prions stay deadly despite sticking to soil comes as a surprise, because while many proteins can bind to soil, that binding usually changes their shapes and activities. The scientists suggest that certain soil types serve as natural prion repositories in the wild. As animals regularly consume soil to meet their mineral needs, it's possible that prion−laden soil particles contribute to the transmission of prion disease such as CWD among animals. CWD is

a fatal, incurable condition that belongs to a family of prion−inflicted neurological disorders known as transmissible spongiform encephalopathies. Originally detected in the 1960s in Colorado and Wyoming, CWD is now present in 14 states and two Canadian provinces. Prions are an incorrectly folded variation of a protein normally found in mammals, including humans. Prions Adhere to Soil Minerals and Remain Infectious: http://pathogens.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.ppat.0020032
Source: http://www.news.wisc.edu/12428.html

21. *April 13, Canadian Food Inspection Agency* — **Potential case of bovine spongiform encephalopathy identified in Canada.** The Canadian Food Inspection Agency (CFIA) is currently conducting confirmatory testing of samples from a cow from British Columbia suspected of having bovine spongiform encephalopathy (BSE). No part of the animal−an approximately six−year−old dairy cow−entered the human food or animal feed systems, and the entire carcass has been placed under control. The cow was identified on a Fraser Valley farm through the national BSE surveillance program. Since detecting Canada's first case in 2003, Canada's surveillance program, which targets animals most at risk of having BSE, has tested approximately 100,000 animals. After initial screening tests conducted provincially produced inconclusive results, samples from the animal were sent to the National Center for Foreign Animal Disease in Winnipeg for further analysis. The first part of this process has been completed and produced a preliminary positive result. Final testing is now underway. The age of this animal would be consistent with previous cases and exposure to a low level of BSE infectivity.
Source: http://www.inspection.gc.ca/english/corpaffr/newcom/2006/200 60413e.shtml

[Return to top]

Food Sector

22. *April 14, Arirang News (South Korea)* — **South Korea to decide on U.S. beef import this month.** The Korean government may resume U.S. beef imports as early as May once officials here confirm the exact age of an Alabama cow which tested positive for mad cow disease in March. Korea's Ministry of Agriculture and Forestry says Korean veterinarians will examine if the cow in question was born before 1998 based on information provided by the U.S. government. The birth date is significant because Korea has agreed it will only re−impose a ban on U.S. beef when the disease is detected in cattle born after April 1998.
Source: http://english.chosun.com/w21data/html/news/200604/200604140 023.html

23. *April 13, Reuters* — **U.S. fails to meet goal on Listeria as rate rises.** The U.S. fell short of its 2005 goal to reduce cases of the foodborne bacteria Listeria by 50 percent. The U.S. Centers for Disease Control and Prevention said the rate of Listeria food poisoning rose in 2005 to three cases per million people, an increase from 2.7 cases per million a year earlier. Listeria is a potentially fatal disease for at−risk populations including the very young and elderly. It can cause high fever, severe headache and nausea. U.S. health officials say it triggers about 2,500 illnesses each year and 500 deaths. As recently as 1998 the rate was near five cases per million.
Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyid=2006−04−13T221401Z_01_N13294519_RTRUKOC_0_US−FO

OD−LISTERIA.xml

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

24. *April 16, Agence France−Presse* — **Pakistan reports third bird flu outbreak.** The Pakistani authorities have reported the country's third outbreak of the H5N1 strain of bird flu at a chicken farm near the capital Islamabad. "We found some 3,600 birds dead at the farm on Friday, April 14. We collected samples and conducted tests," said Mohammad Afzal, spokesperson for the Food, Agriculture and Livestock Ministry. The H5N1 strain was found at a farm in Sihala town, Afzal said.
Source: http://www.forbes.com/finance/feeds/afx/2006/04/16/afx267272 6.html

25. *April 16, Associated Press* — **Bangladesh confirms first polio case in six years.** Bangladesh confirmed on Friday, April 14, the country's first case of polio in nearly six years, prompting plans to resume mass vaccinations against the crippling disease next month. Laboratory tests showed that a 9−year−old girl in the eastern Chandpur district, has polio, health officials said. “We are worried,” said Arun Thapa, the World Health Organization's regional adviser for polio in Southeast Asia who investigated the case. “The virus has had time to spread.” The girl came in contact with a family who had recently visited India's Uttar Pradesh state, where polio is endemic. Bangladesh had been polio−free since August 2000 thanks to extensive vaccination. Polio is endemic in only four countries –− Afghanistan, India, Nigeria and Pakistan. The disease is also present in eight other countries −– including Yemen, Indonesia and Somalia −– where it had previously been eradicated before being imported again from one of the endemic countries.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.signonsandiego.com/news/world/20060317−1107−bangl adesh−polio.html

26. *April 16, Washington Post* — **U.S. plan for flu pandemic revealed.** President Bush is expected to approve soon a national pandemic influenza response plan that identifies more than 300 specific tasks for federal agencies, including determining which frontline workers should be the first vaccinated and expanding Internet capacity to handle what would probably be a flood of people working from their home computers. The Treasury Department is poised to sign agreements with other nations to produce currency if U.S. mints cannot operate. The Pentagon, anticipating difficulties acquiring supplies from the Far East, is considering stockpiling millions of latex gloves. And the Department of Veterans Affairs has developed a drive−through medical exam to quickly assess patients who suspect they have been infected. The document is the first attempt to spell out in some detail how the government would detect and respond to an outbreak, and continue functioning through what could be an 18−month crisis. In response to questions posed to several federal agencies, White House officials offered a briefing on the

near−final version of its 240−page plan.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/15/AR2006041500901_pf.html

27. *April 15, New York Times* — **Bird flu virus may be spread by smuggling.** There is increasing evidence that a thriving international trade in smuggled poultry−−including live birds, chicks and meat−−is helping spread bird flu, experts say. Poultry smuggling is a huge business that poses a unique threat: The (A)H5N1 bird flu virus is robust enough to survive not just in live birds but also in frozen meat, feathers, bones and even on cages, though it dies with cooking. Poultry from bird−flu−infected countries has been banned in Europe since 2002, but smuggling seriously undermines those bans. "In spite of the E.U. ban, we are still seizing Chinese poultry products," said Gen. Emilio Borghini, commander of the Military Police Health Service in Italy. There is extensive smuggling between China and Africa. In the developing world, the illegal trade often has economic roots, to avoid duties. The trade is hard to control because huge amounts cross borders in trucks, carts, planes and boats each day. Smuggled meat from Asia is often loaded in containers with a mishmash of other goods, like clothes, toys and furniture.
Source: http://www.nytimes.com/2006/04/15/world/europe/15bird.html?ei=5065&en=e1e386d4eaff5831&ex=1145764800&partner=MYWAY&pagew anted=print

28. *April 14, U.S. Centers for Disease Control and Prevention* — **Multi−state mumps outbreak.** The state of Iowa has been experiencing a large outbreak of mumps that began in December 2005. As of April 12, 2006, 605 suspect, probable and confirmed cases have been reported to the Iowa Department of Public Health. The majority of cases are occurring among persons 18−25 years of age, many of whom are vaccinated. Additional cases of mumps, possibly linked to the Iowa outbreak, are also under investigation in eight neighboring states, including Illinois, Indiana, Kansas, Michigan, Minnesota, Missouri, Nebraska, and Wisconsin. In addition, the Iowa Department of Public Health has identified two persons diagnosed with mumps who were potentially infectious during travel on nine different commercial flights involving two airlines between March 26, 2006 and April 2, 2006. The origin and arrival cities for these flights include Cedar Rapids and Waterloo, IA; Dallas, TX; Detroit, MI; Lafayette, AR; Minneapolis, MN; St. Louis, MO; Tucson, AZ; and Washington, DC. The source of the current U.S. outbreak is unknown. However the mumps strain has been identified as genotype G, the same genotype circulating in the United Kingdom (UK). The outbreak in the UK has been ongoing from 2004 to 2006 and has involved over 70,000 cases.
Iowa Department of Public Health: http://www.idph.state.ia.us/adper/mumps.asp
Source: http://www.phppo.cdc.gov/HAN/ArchiveSys/ViewMsgV.asp?AlertNu m=00243

29. *April 13, Agence France−Presse* — **Egypt reports fourth bird flu death.** An 18−year−old Egyptian girl died of the H5N1 strain of bird flu, the fourth fatal case in the country, a health official announced. Egypt announced on Tuesday, April 11, that the teenager from the northern governorate of Menufiya had been taken to hospital four days earlier. She was the 12th Egyptian infected by the pathogenic virus. The woman is said to have contracted the disease after handling infected poultry. Egypt, the most populous country in the Arab world, is on a major route for migratory birds and is the hardest−hit non−Asian country since the bird flu epidemic broke out in 2003. It was first detected in birds in Egypt in February. The first human case was reported on March 18. Of the 12 Egyptians infected over the past weeks, four have died, five have recovered and three are receiving treatment, health officials said.

Source: http://news.yahoo.com/s/afp/20060413/wl_mideast_afp/healthfluegypt_060413201706;_ylt=Au.7D9Bt0kcDJ6Wq69Y84zuJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

30. *April 13, Maryland Coast Dispatch* — **Maryland courthouse bomb threat: Third of its kind received in a month.** Regular business in Snow Hill, MD, was interrupted for the third time in a month last week when the Worcester County Government Center was forced to evacuate after receiving a bomb threat on Tuesday morning, April 11. Nothing was found. Consequently, this event was the third of its kind in the last month in Snow Hill, joining a suspicious call made to the same facility on March 10 and a bomb threat made to the nearby local branch of the Mercantile Peninsula Bank on March 13, both of which also found no explosives or suspicious materials during the searches.
Source: http://www.mdcoastdispatch.com/calls041406.html

31. *April 13, Mercury News (CA)* — **California federal building reopens after bomb scare.** The federal building in downtown San Jose, CA, was evacuated for more than three hours Thursday, April 13, after an employee found a suspicious package that was eventually blown up by a police bomb squad. The federal building complex was cleared around 1 p.m. PDT, shutting down the federal courts for the afternoon. Meanwhile, the bomb scare disrupted pedestrian traffic, as well as public transportation through the downtown corridor.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/the_valley/14336676.htm

[Return to top]

Emergency Services Sector

32. *April 13, Long Island Business News* — **Long Island: Readying for hurricane season.** Suffolk County, NY, Executive Steve Levy there are many holes left in the region's preparedness. To that end, Levy outlined a 19−point action plan to clean up questions regarding evacuation procedures, communications, transportation, and necessary supplies. The action plan calls for government officials to report back to address readiness concerns by June. In addition, the region is planning an Island−wide drill in June to simulate how the region would respond to a severe hurricane.
Source: http://www.libn.com/breakingNews.htm?articleID=4750

33. *April 13, Government Technology* — **Ohio top officials participate in pandemic flu exercise.** Ohio Governor Bob Taft will meet with key state agency officials and representatives of the poultry industry to discuss the state's preparedness for a potential outbreak of highly pathogenic avian influenza in waterfowl or commercial poultry. The discussion will include how emergency responders would handle an incursion of avian influenza in commercial poultry flocks and birds in the wild and how the state would communicate with the public. Top officials

from the following agencies will participate in the exercise: the Ohio Departments of Administrative Services, Agriculture, Environmental Protection Agency, Health, Natural Resources and Public Safety and the Ohio Emergency Management Agency, State Veterinarian and Ohio Poultry Association.
Source: http://www.govtech.net/magazine/channel_story.php/99178

[Return to top]

Information Technology and Telecommunications Sector

34. *April 13, FrSIRT* — **Mozilla products memory corruption and information disclosure vulnerabilities.** Multiple vulnerabilities have been identified in Mozilla Firefox, Mozilla Suite, SeaMonkey, and Thunderbird, which may be exploited by remote attackers to take complete control of an affected system, bypass security restrictions, or disclose sensitive information. For details on the 22 flaws outlined by FrSIRT, please see source advisory. Vulnerable products: Firefox versions prior to 1.5; Firefox versions prior to 1.0.8; Mozilla Suite versions prior to 1.7.13; SeaMonkey versions prior to 1.0; Thunderbird versions prior to 1.5.0.2; Thunderbird versions prior to 1.0.8.
Solution: Upgrade to Firefox 1.5 or 1.0.8: http://www.mozilla.com/firefox/
Upgrade to Mozilla Suite 1.7.13: http://www.mozilla.org/products/mozilla1.x/
Upgrade to SeaMonkey 1.0: http://www.mozilla.org/projects/seamonkey/
Upgrade to Thunderbird 1.5.0.2 or 1.0.8: http://www.mozilla.com/thunderbird/
Source: http://www.frsirt.com/english/advisories/2006/1356

35. *April 13, Security Focus* — **Apache HTTP request smuggling vulnerability.** Apache is prone to an HTTP request smuggling attack. Analysis: A specially crafted request with a "Transfer Encoding: chunked" header and a "Content Length" header can cause the server to forward a reassembled request with the original "Content Length" header. As a result, the malicious request may piggyback on the valid HTTP request. This attack may result in cache poisoning, cross site scripting, session hijacking, and other attacks. If the described issues have been exploited to cause a denial−of−service condition, the Apache Web Server may be slow to respond to requests or may not respond at all. There are no predictable symptoms that would indicate any of the described issues have been exploited to gain unauthorized access to a host or its data. For a complete list of vulnerable products:
http://www.securityfocus.com/bid/14106/info
Solution: The vendor has released Apache 2.1.6 to address this issue in the 2.1.x branch. The vendor addressed this issue for earlier versions as well: version 2.0.55 of the 2.0 branch and version 1.3.34 of the 1.3 branch.
Please see the referenced vendor advisories for further information:
http://www.securityfocus.com/bid/14106/references
Source: http://www.securityfocus.com/bid/14106/discuss

36. *April 13, Security Focus* — **Apache mod_ssl CRL handling off by one buffer overflow vulnerability.** Apache's mod_ssl is prone to an off by one buffer overflow condition. The vulnerability arising in the mod_ssl CRL verification callback allows for potential memory corruption when a malicious CRL is handled. Analysis: Several vulnerabilities in the Apache 2.0 Web server prior to version 2.0.55 may allow a local or remote unprivileged user to cause a

denial−of−service to the Apache 2 HTTP process, or may allow a local user who is able to write to directories served by the Web server to execute arbitrary code with the privileges of the Apache 2 process. The Apache 2 HTTP process normally runs as the unprivileged user "webservd" (uid 80). For a complete list of vulnerable products: http://www.securityfocus.com/bid/14366/info
Solution: The vendor has addressed this issue in version 2.0.55 of the 2.0 branch. Users are advised to obtain the available update.
Please see the referenced vendor advisories for further information: http://www.securityfocus.com/bid/14366/references
Source: http://www.securityfocus.com/bid/14366/discuss

37. *April 13, Security Focus* — **Adobe Document Server for Reader Extensions multiple remote vulnerabilities.** Adobe Document Server for Reader Extensions, included with Graphics Server and Document Server, is prone to multiple vulnerabilities. Analysis: When using Adobe Document Server for Reader Extensions 6.0, a user's session ID is included in the URL ("jsessionid" parameter) and is exposed to other Websites in the "Referer:" header. It is possible that a malicious person might monitor a company's Internet traffic to steal the sessionid directly from the URL. That session ID could be used by the malicious person to gain a copy of the PDF file that a legitimate user is processing with Reader Extensions. Vulnerable products: Adobe Graphics Server 2.1 and Adobe Document Server 6.0.
Solution: Adobe has released advisories and updated software to address these issues.
Please see the referenced advisories for further information:
http://www.securityfocus.com/bid/17500/references
Source: http://www.securityfocus.com/bid/17500/discuss

38. *April 13, MSNBC* — **Portable computer drives peddled at bazaar outside Bagram Air Base, Afghanistan.** This week in Bagram, Afghanistan, an NBC News producer, using a hidden camera, visited a bazaar and bought a half dozen of the memory drives the size of a thumb known as flash drives. Some of the discovered data would be valuable to the enemy, including: Names and personal information for dozens of Department of Defense interrogators; documents on an "interrogation support cell" and interrogation methods; IDs and photos of U.S. troops. The tiny computer memories are believed to have been smuggled off base by Afghan employees and sold to shopkeepers. Whoever buys one can simply plug it into another computer, and in a couple of minutes, see thousands of files.
Source: http://www.msnbc.msn.com/id/12305580/

39. *April 13, ZDNet (UK)* — **NASA hacker to speak at security show.** NASA hacker Gary McKinnon will be joined by other hackers and security experts on a panel discussion at the Infosecurity Europe conference Thursday, April 27, in London. McKinnon faces the prospect of an indefinite stay in Guantanamo Bay, but this won't prevent him from appearing on the Infosecurity panel and discussing hacking at a UK security conference. The NASA hacker is currently fighting extradition to the U.S. in what has been a protracted trial. He is charged with gaining unauthorized access to 97 U.S. government computers, including machines belonging to NASA and the Department of Defense. He claims he was searching for evidence of UFOs.
Source: http://news.zdnet.co.uk/internet/security/0,39020375,3926334 1,00.htm

40.

April 12, Kaspersky Lab — **Kaspersky Lab has released quarterly malware evolution report.** Kaspersky Lab has released its quarterly analysis report for January−March 2006 on malware evolution. The report contains details of IT security events which occurred in the first quarter of 2006, and which are likely to influence the future evolution of malicious code and cyber threats. The report is intended for IT security professionals and users with an interest in malicious code. For the full report, please refer to the source.
Source: http://www.viruslist.com/en/analysis?pubid=184012401

41. *April 12, Security Focus* — **Browser crashers warm to data fuzzing.** Last month, security researcher HD Moore decided to write a simple program that would mangle the code found in Webpages and gauge the effect such data would have on the major browsers. The result: hundreds of crashes and the discovery of several dozen flaws. The technique −− called packet, or data, fuzzing −− is frequently used to find flaws in network applications. Moore and others are now turning the tool on browsers to startling results. In a few weeks, the researcher had found hundreds of ways to crash Internet Explorer and, to a lesser extent, other browsers. In another example, it took less than an hour at the CanSecWest Conference last week for Moore and information−systems student Matthew Murphy to hack together a simple program to test a browser's handling of cascading style sheets, finding another dozen or so ways to crash browsers. "Fuzzing is probably the easiest way to find flaws, because you don't have to figure out how the application is dealing with input," said Moore, a well−known hacker and the co−founder of the Metasploit Project.
Source: http://www.securityfocus.com/news/11387

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of an active exploitation of a cross site scripting vulnerability in the eBay website. Successful exploitation may allow an attacker to take various actions, including the following:

Obtain sensitive data from stored cookies Redirect auction viewers to phishing sites where further disclosure of login credentials or personal information can occur Create auctions that use script to place login areas on the eBay website, where credentials may be sent to a remote server with malicious intent

For more information please review the following advisory and vulnerability notes:

CA−2000−02 − Malicious HTML Tags Embedded in Client Web Requests.
http://www.cert.org/advisories/CA−2000−02.html

VU#808921 − eBay contains a cross−site scripting vulnerability.
http://www.kb.cert.org/vuls/id/808921

US−CERT recommends the following:

Securing Your Web Browser
http://www.us−cert.gov/reading_room/securing_browser/#how_to _secure

Malicious Web Scripts FAQ
.http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

eBay Spoof Email Tutorial
http://pages.ebay.com/education/spooftutorial/spoof_3.html

US−CERT Cyber Security Tip ST04−014.
http://www.us−cert.gov/cas/tips/ST04−014.html

Cyber Security Tip ST05−010. http://www.us−cert.gov/cas/tips/ST05−010.html

Add "ebay.com" to the Restricted Sites zone in Internet Explorer.

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 32459 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 25 (smtp), 32768 (HackersParadise), 135 (epmap), 6346 (gnutella−svc), 139 (netbios−ssn), 1434 (ms−sql−m) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

42. *April 14, Western Courier (IL)* — **Western Illinois University main administration building shut down due to bomb scare.** A bomb scare had Western Illinois University's main administration building shut down for three hours Thursday morning, April 13. More than 200 employees working in Sherman Hall were forced to evacuate the building due to a suspicious

package found outside the front entrance of the building. The message on the package warned to contact the Office of Public Safety. The package turned out to contain a piece of audio−visual equipment.
Source: http://www.westerncourier.com/media/storage/paper650/news/2006/04/14/News/Sherman.Hall.Package.Scare−1852149.shtml?norewrite200604141444&sourcedomain=www.westerncourier.com

43. *April 14, Whittier Daily News (CA)* — **School evacuated after pipe bomb found.** Deputies evacuated the Holy Name of Mary School and 20 nearby residents in San Dimas, CA, Wednesday, April 12, after a pipe bomb was found on campus. The sheriff's Arson and Explosive Unit rendered the device harmless. However, it was later determined to be a live bomb.
Source: http://www.whittierdailynews.com/news/ci_3704526

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.